NAT64/464XLAT Deployment Guidelines in Operator and Enterprise Networks

draft-ietf-v6ops-nat64-deployment-03

Jordi Palet
jordi.palet@theipv6company.com
History

• Discussion in IETF regarding using only NAT64 in our network
• Suggested deploying 464XLAT instead
• Discussion: DNS64 breaks DNSSEC
  • 464XLAT can be used w/o DNS64, which is not possible for (only) NAT64
    – Document presented in IETF 100
• WG suggested to be an “overall” NAT64 deployment guidelines document
What is/What is not this doc

• Not a discussion of NAT64 vs other transition mechanisms

• Not just discussing about DNSSEC, however is key

• If you already decided to go for something based in NAT64, here are your choices (section 3. Scenarios) and what you should take care about (section 4. Issues)
1. Introduction

• 3 issues
  – DNS64 may break DNSSEC
    • Small %, may be ok in some cases (cellular, no validation)
  – NAT64/DNS64 don’t work with literals and older APIs
    • Sorted out partially with Happy Eyeballs v2
  – NAT64, alone doesn’t work for IPv4-only hosts/apps
    • This may be ok in some scenarios (cellular), unless there is a need for IPv4 (example, tethering)
3. NAT64 Deploy. Scenarios

• Since DNS64 was published (with 3 scenarios), there are new ones to consider

• For an operator, the network should work in all the cases

• Scenarios described in two groups:
  – known to work
  – known to work under special conditions
3.1. Known to Work

3.1.1. Service provider NAT64 with DNS64
   – Internal or outsourced (NAT64 / DNS64)
   – 4 possible sub-scenarios (1-4)

3.1.2. 464XLAT with DNS64
   – Internal or outsourced (NAT64 / DNS64)
   – 3 possible sub-scenarios (5-7)

3.1.3. 464XLAT without DNS64
   – Internal or outsourced (NAT64)
   – 2 possible sub-scenarios (8-9)
3.2. Known to Work Under Special Conditions

3.2.1. Service provider NAT64 without DNS64
   – Sub-scenario 10

3.2.2. Service provider NAT64
   DNS64 in the IPv6 hosts
   – Sub-scenario 11

3.2.3. Service provider NAT64
   DNS64 in the remote IPv4-only network
   – Sub-scenario 12
3.3. Comparing Scenarios

a. DNSSEC: Are there hosts validating?
b. Literal/APIs: Are being used?
c. IPv4-only: Any IPv4-only usage?
d. Foreign DNS: Is the scenario surviving?

Rate each item per scenario as good (+) or bad (-)
4. Issues to be Considered (1)

4.1. DNSSEC Considerations & Approaches
   4.1.1. Not using DNS64
   4.1.2. DNSSEC validator aware of DNS64
   4.1.3. Stub validator
   4.1.4. CLAT with DNS proxy and validator
   4.1.5. ACL of clients
   4.1.6. Mapping-out IPv4 addresses

4.2. DNS64 reverse mapping considerations

4.3. Using 464XLAT with/without DNS64
4. Issues to be Considered (2)

4.4. Manual configuration of “foreign” DNS
4.5. DNS Privacy
4.6. Split DNS
4.7. Well-Known Prefix (WKP) vs Network-Specific Prefix (NSP)
4.8. IPv4 literals and old APIs
4.9. IPv4-only hosts or apps
4.10. CLAT translation considerations
Other Sections

5. Summary of Deployment Recommendations for NAT64
6. Deployment of NAT64 in Enterprise Networks

...  
10. ANNEX A: Example of Broadband Deployment with 464XLAT
11. ANNEX B: CLAT Implementation
12. ANNEX C: Benchmarking
Next steps

• Questions ?

• Inputs ?